

WHAT IS CLAIMED IS:

1 1. A system for securely transmitting Real Time Protocol voice packets
2 during a communication session with a remote multimedia terminal adapter over an Internet
3 protocol network, the system comprising:

4 a local multimedia terminal adapter receiving the voice packets, the local
5 multimedia terminal adapter comprising,

6 a local key stream generator for generating a first key stream;

7 a packet encryptor that encrypts the voice packets using at least a
8 portion of the first key stream to form encrypted voice packets;

9 the remote multimedia terminal adapter receiving the encrypted voice
10 packets, the remote multimedia terminal adapters further comprising,

11 a remote key stream generator for generating the first key stream in
12 order to decrypt the encrypted voice packets; and

13 a packet decryptor decrypting the encrypted voice packets using the
14 first key stream, wherein both key stream generators are capable of generating a second key
15 stream to prevent reuse of any portion of the first key stream during the communication
16 session.

1 2. The system of claim 1 wherein the second key stream is generated
2 when the system wishes to switch from a first to a second coder/decoder for
3 compression/decompression of the voice packets.

1 3. The system of claim 1 wherein the second key stream is generated
2 when a Message Authentication Code algorithm change occurs.

1 4. The system of claim 1 further comprising a local gateway controller
2 for forwarding the encrypted packets through the Internet protocol network.

1 5. The system of claim 1 further comprising a remote gateway controller
2 for receiving the encrypted packets from the Internet protocol network and for forwarding
3 encrypted voice packets to the remote multimedia terminal adapter.
4

1 5. A system for communicating Real Time Protocol voice packets
2 between a local and a remote location over an Internet protocol network, the system
3 comprising:
4 a stream cipher module for encrypting the voice packets; and
5 a key stream generator for generating a first Real Time Protocol key stream,
6 the stream cipher module employing the first key stream to encrypt the voice packets for
7 forwarding to the remote location, the key stream generator producing a second Real Time
8 Protocol key stream for encrypting the voice packets when the system wishes to switch from
9 a first communication parameter to a second communication parameter, each of the first and
10 second parameters being involved in the synchronization of the key stream.

1 6. The system of claim 6 wherein the first communication parameter is a
2 first coder/decoder that compresses/decompresses the voice packets, and the second
3 communication parameter is a second coder/decoder that compresses/decompresses the voice
4 packets.

1 7. The system of claim 6 further comprising a synchronization source for
2 synchronizing and enabling decryption of the voice packets at the remote location.

1 8. The system of claim 8 wherein the synchronization source is a time
2 stamp on a voice packet.

1 9. The system of claim 9 further comprising a new time stamp sequence
2 generated when the second Real Time Protocol key stream is generated.

1 10. The system of claim 6 wherein the second key stream is generated by
2 re-executing the following key derivation function:

3 F(S, "End-End RTP Key Change <N>")

4 where N is a counter incremented whenever a new set of Real Time Protocol
5 keys is re-derived for the same media stream session;

6 F() is a one-way pseudo-random function used for the purpose of key
7 derivation;

8 S is a shared secret - a random value shared between the two endpoints and is
9 known only to those two endpoints and possibly a trusted server (e.g. gateway controller);

10 and

11 "End-End RTP Key Change <N>" is a label that is used as a parameter to the
12 key derivation function F(), <N> stands for an ASCII representation of a decimal number,
13 representing a counter.

1 11. The system of claim 6 wherein the second key stream is generated by
2 re-executing the following key derivation function:

3 F(S, SSRC, "End-End RTP Key Change <N>") where:

4 S is a shared secret - a random value shared between the two endpoints and is
5 known only to those two endpoints and possibly a trusted server (e.g. gateway controller);

6 SSRC is the synchronization source session identifier;

7 N is the counter of the number of key changes for the same SSRC value; and

8 "End-End RTP Key Change <N>" is a label that is used as a parameter to the
9 key derivation function F(), <N> stands for an ASCII representation of a decimal number,
10 representing a counter.

1 12. A method for securely transmitting Real Time Protocol voice packets
2 from a local to a remote location via a communication network, the method comprising:

3 generating a first Real Time Protocol key stream for encrypting the voice
4 packets;

5 forwarding encrypted voice packets to the remote location;

6 generating a second Real Time Protocol key stream for encrypting the voice
7 packets in response to a request to change communication parameters for the same media
8 stream; and

9 forwarding voice packets encrypted with the second Real Time Protocol key
10 stream to the remote location.

1 13. The method of claim 13 further comprising reinitializing a time stamp
2 for synchronizing decryption of the voice packets.

1 14. The method of claim 13 wherein the step of generating a second Real
2 Time Protocol key stream is by re-executing the following key derivation function:

3 F(S, "End-End RTP Key Change <N>")

4 where N is a counter incremented whenever a new set of Real Time Protocol
5 keys is re-derived for the same media stream session;

6 F() is a one-way pseudo-random function used for the purpose of key
7 derivation;;
8 S is a shared secret - a random value shared between the two endpoints and is
9 known only to those two endpoints and possibly a trusted server (e.g. gateway controller);
10 and
11 "End-End RTP Key Change <N>" is a label that is used as a parameter to the
12 key derivation function F(), <N> stands for an ASCII representation of a decimal number,
13 representing a counter.

1 15. The method of claim 13 wherein the step of generating a second Real
2 Time Protocol key stream is by re-executing the following key derivation function:

3 F(S, SSRC, "End-End RTP Key Change <N>") where:
4 S is a shared secret - a random value shared between the two endpoints and is
5 known only to those two endpoints and possibly a trusted server (e.g. gateway controller);
6 SSRC is the synchronization source session identifier;
7 N is the counter of the number of key changes; and
8 "End-End RTP Key Change <N>" is a label that is used as a parameter to the
9 key derivation function F(), <N> stands for an ASCII representation of a decimal number,
10 representing a counter.

1 16. In a communication system having a gateway receiving
2 communication sessions from two or more multimedia terminal adapters, a method for
3 securely exchanging voice packets between the multimedia terminal adapters and the
4 gateway, the method comprising:
5 generating a first Real Time Protocol key stream for encrypting the voice
6 packets;
7 forwarding the voice packets encrypted with the first Real Time Protocol key
8 stream to the gateway;
9 generating a second Real Time Protocol key stream for encrypting the voice
10 packets in response to a collision detection wherein the multimedia terminal adapters have
11 the same source identifier; and
12 forwarding voice packets encrypted with the second Real Time Protocol key
13 stream to the remote location.

1 17. The method of claim 17 wherein the step of generating a second Real
2 Time Protocol key stream is by re-executing the following key derivation function:

3 F(S, SSRC, "End-End RTP Key Change <N>") where:

4 S is a shared secret - a random value shared between the two endpoints and is
5 known only to those two endpoints and possibly a trusted server (e.g. gateway controller);

6 SSRC is the synchronization source session identifier;

7 N is the counter of the number of key changes; and

8 "End-End RTP Key Change <N>" is a label that is used as a parameter to the
9 key derivation function F(), <N> stands for an ASCII representation of a decimal number,
10 representing a counter.

1 18. A system for securely transmitting voice packets during a
2 communication session from a local location to a remote location over a communication
3 network, the system comprising:

4 a means for generating a first key stream at the local location;

5 a means for encrypting the voice packets using at least a portion of the first
6 key stream to form encrypted voice packets;

7 a means for forwarding the encrypted voice packets from the local location to
8 the remote location;

9 a means for generating the first key stream at the remote location in order to
10 decrypt the encrypted voice packets; and

11 a means for decrypting the encrypted voice packets using the first key stream,
12 wherein both means for generating are capable of generating a second key stream to prevent
13 reuse of any portion of the first key stream during the communication.

1 19. The system of claim 19 wherein the second key stream is generated
2 when the system wishes to switch from a first to a second coder/decoder for
3 compression/decompression of the voice packets.

1 20. The system of claim 19 wherein the second key stream is generated by
2 re-executing the following key derivation function:

3 F(S, "End-End RTP Key Change <N>")

4 where N is a counter incremented whenever a new set of Real Time Protocol
5 keys is re-derived for the same media stream session;

6 F() is a one-way pseudo-random function used for the purpose of key
 7 derivation;
 8 S is a shared secret - a random value shared between the two endpoints and is
 9 known only to those two endpoints and possibly a trusted server (e.g. gateway controller);
 10 and
 11 "End-End RTP Key Change <N>" is a label that is used as a parameter to the
 12 key derivation function F(), <N> stands for an ASCII representation of a decimal number,
 13 representing a counter.

1 21. The system of claim 19 wherein the second key stream is generated by
 2 re-executing the following key derivation function:
 3 F(S, SSRC, "End-End RTP Key Change <N>") where:
 4 S is a shared secret - a random value shared between the two endpoints and is
 5 known only to those two endpoints and possibly a trusted server (e.g. gateway controller);
 6 SSRC is the synchronization source session identifier;
 7 N is the counter of the number of key changes; and
 8 "End-End RTP Key Change <N>" is a label that is used as a parameter to the
 9 key derivation function F(), <N> stands for an ASCII representation of a decimal number,
 10 representing a counter.

1 22. The system of claim 19 further comprising a means for synchronizing
 2 the voice packets.